

SecuraLive®
INTERNET SECURITY
Home Edition

USER
GUIDE



SECURALIVE®

SECURE AND PROTECT

SecuraLive® INTERNET SECURITY

USER MANUAL

Introduction:

Welcome to SecuraLive® Internet Security Home Edition.

SecuraLive® Internet Security is a collection of high end technologies that work in perfect synergy, having one common goal: to protect your system & network and valuable data against computer viruses. It represents a superior solution for any Windows based workstation.

SecuraLive® Internet Security incorporates Antivirus, Antispyware, Anti Malware & Antiroot kit technology. With firewall & sophisticated protection capabilities Internet Security ensures that your valuable data and programs are always protected. This manual describes the SecuraLive® Internet Security installation and operation. For further options and information, please visit our website:

www.securalive.com

Your SecuraLive® Team.

INSTALLATION

BEFORE STARTING INSTALLATION

- Make sure that no other virus protection solutions are installed.
- The automatic protection functions of various security solutions may interfere with each other.
- Establish an Internet connection for downloading the setup.

INSTALL

The installation program runs in a self-explanatory dialog mode. Every Window contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions.

Go to next step

NEXT

Go to previous step

BACK

To process installation

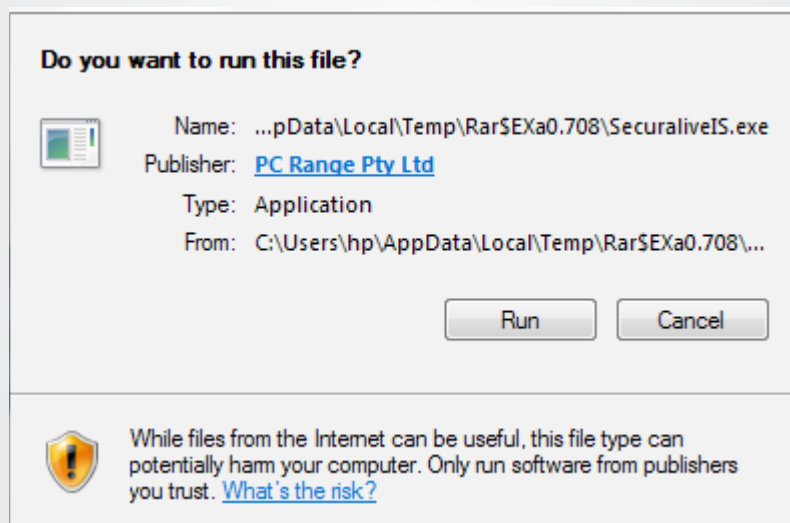
INSTALL

Action finished

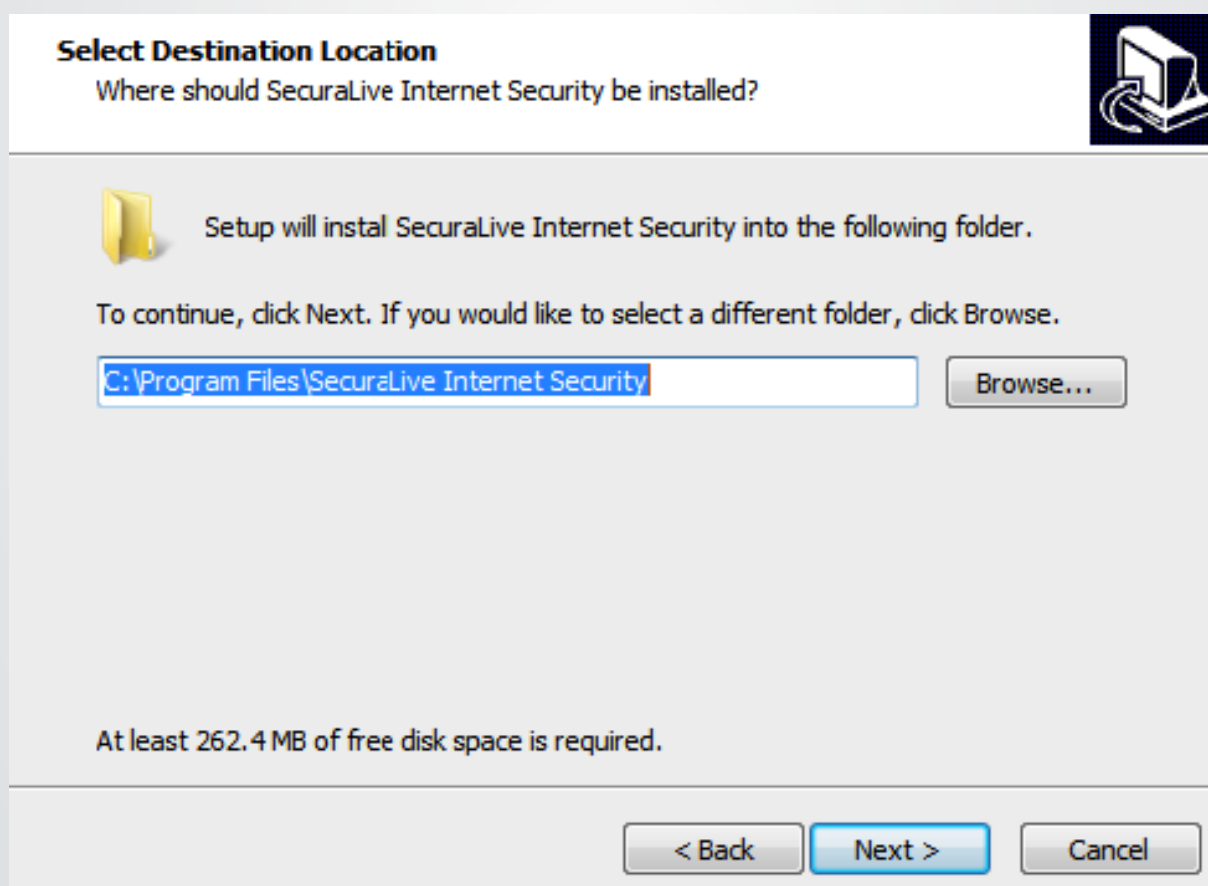
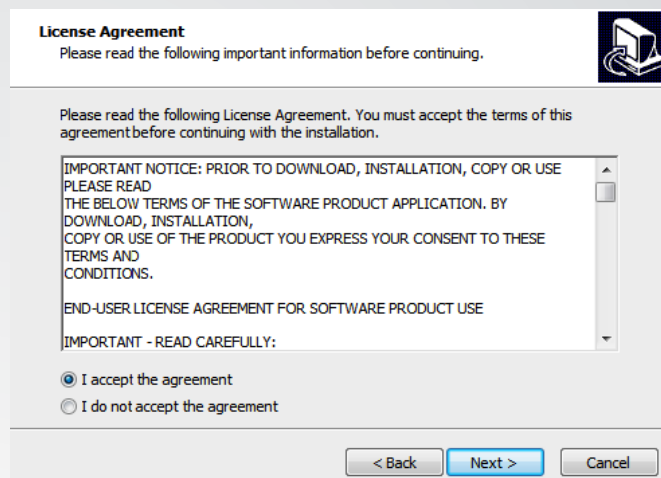
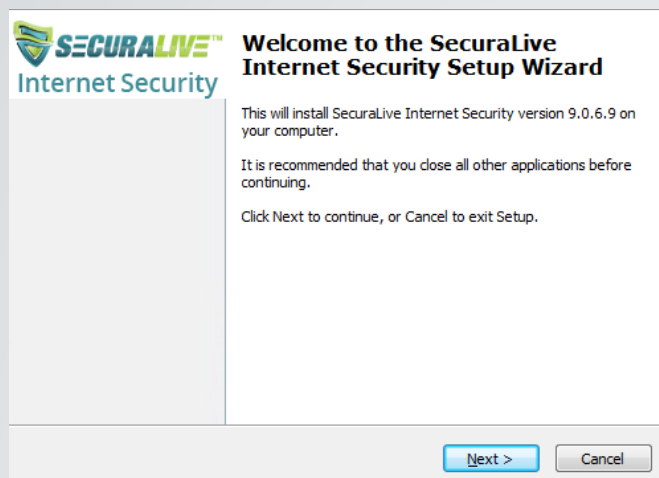
FINISH

INSTALLING YOUR INTERNET SECURITY PROGRAM

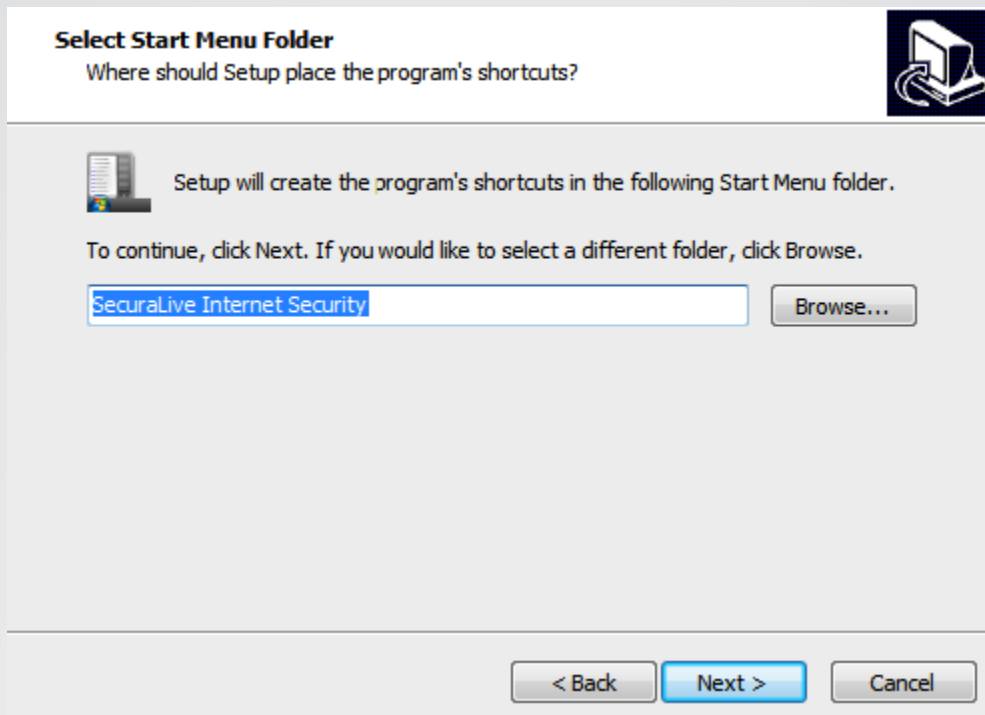
- Install by running the “SecuraLiveIS.exe” installation file by double clicking on it.
- Clicking “Run” will take you to the SecuraLive® Internet Security Setup screen:



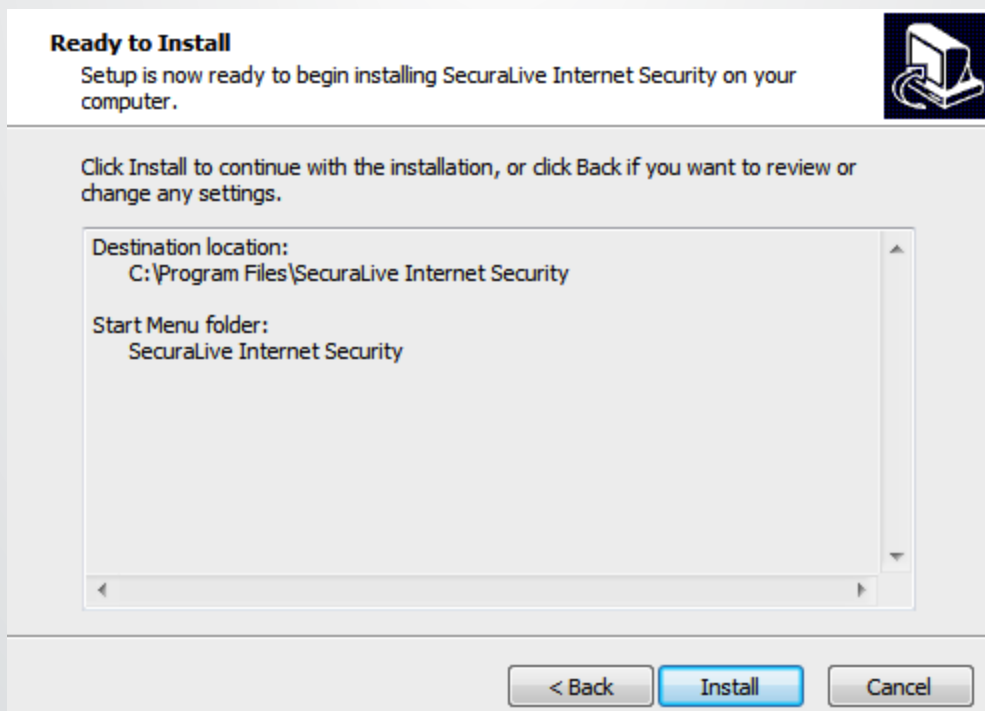
- Click “Next” and the installation Wizard will then guide you through the rest of the installation process.
- First you will be asked to read about the minimum system requirements and then confirm that you agree to the end-user license conditions.
- To continue, click on “I accept the agreement”, this enables “Next” for further steps.



- Clicking on “Next” will navigate you to the destination selection Window.
- You will be asked to confirm the destination directory, i.e. where the program files will be saved. The program will select this automatically or will create a new directory if it doesn't already exist. It is recommended to accept the default destination directory and simply click on “Next” to continue.

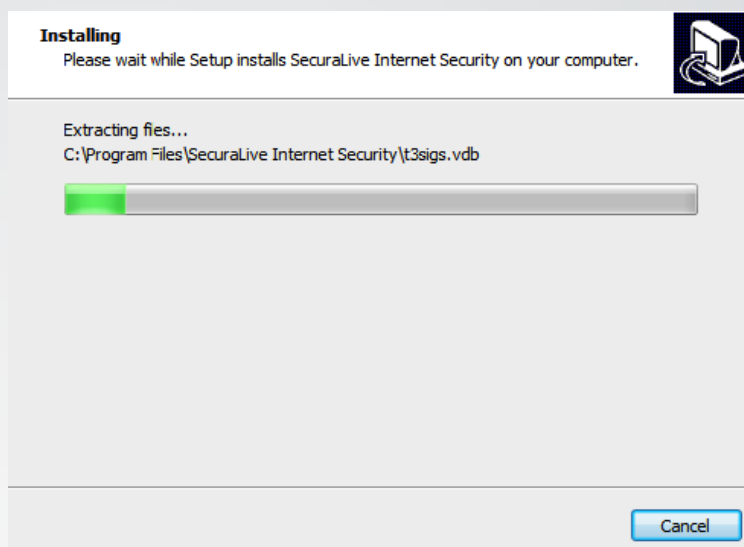


- It will take you to the “Select Start Menu folder” Window to place the program’s shortcuts. By default it will store in the “SecuraLive® Secure” folder, otherwise you can browse a different location. Click on “Next” to continue.



- Now the setup is ready to install the SecuraLive® Internet Security. Click on “Install” for the installation process.

- The installation progress will display as a green progression bar as shown in the screen below.



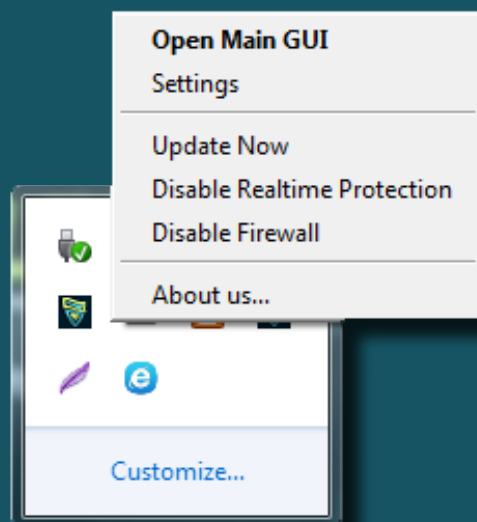
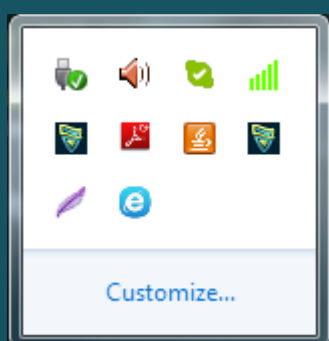
The complete green colored bar confirms that installation has been successfully completed and ensures you with the “Finish” setup wizard.

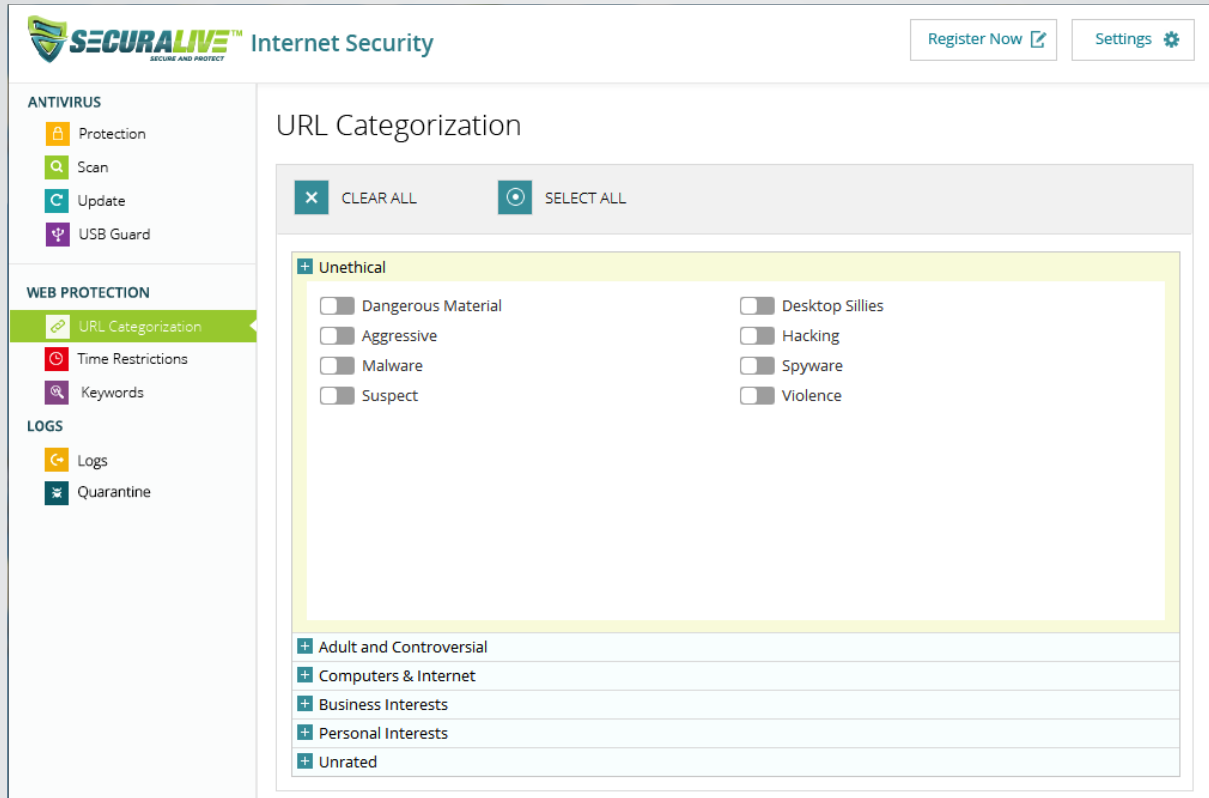
Click on “Finish” to complete the process. With this the installation task has been completed.

WORKING WITH INTERNET SECURITY

After installation a SecuraLive® Internet Security shortcut icon will appear in your taskbar. Click on the icon to see the details of Internet Security.

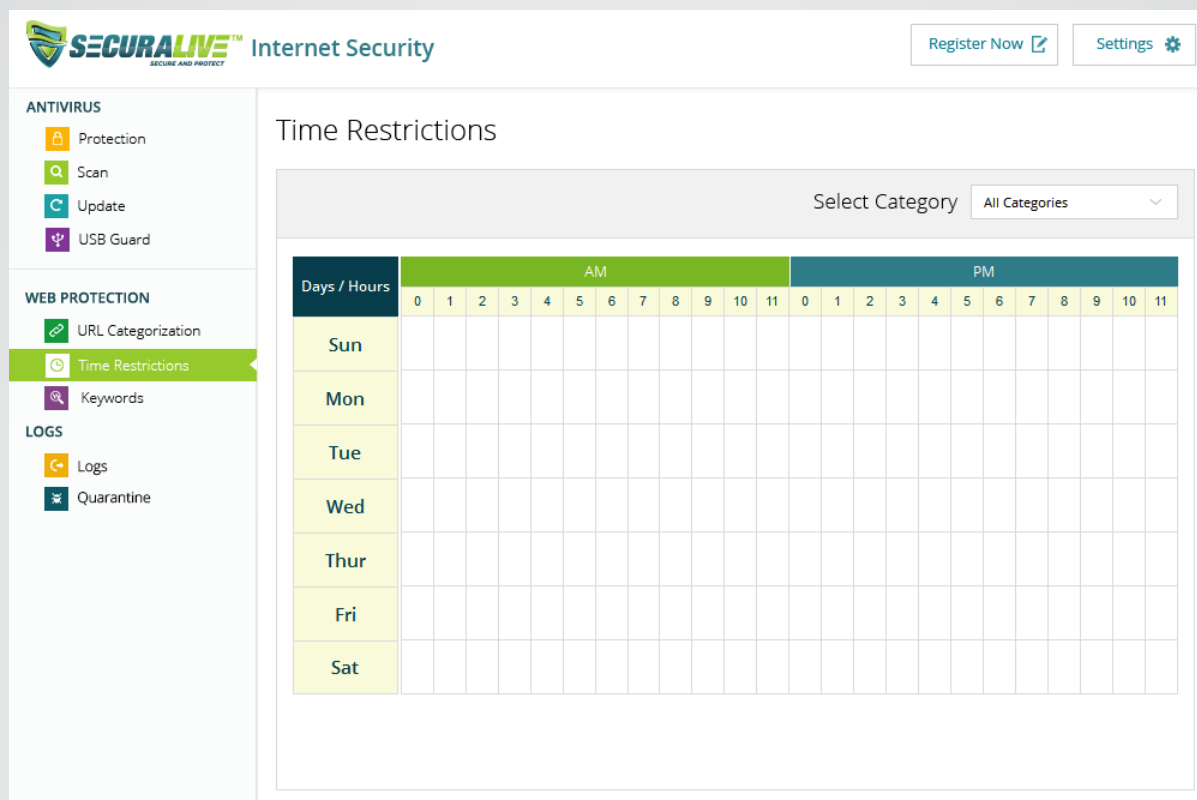
If you right click on that icon it will show options to view the GUI, Update, and Real-time protection options as shown below.





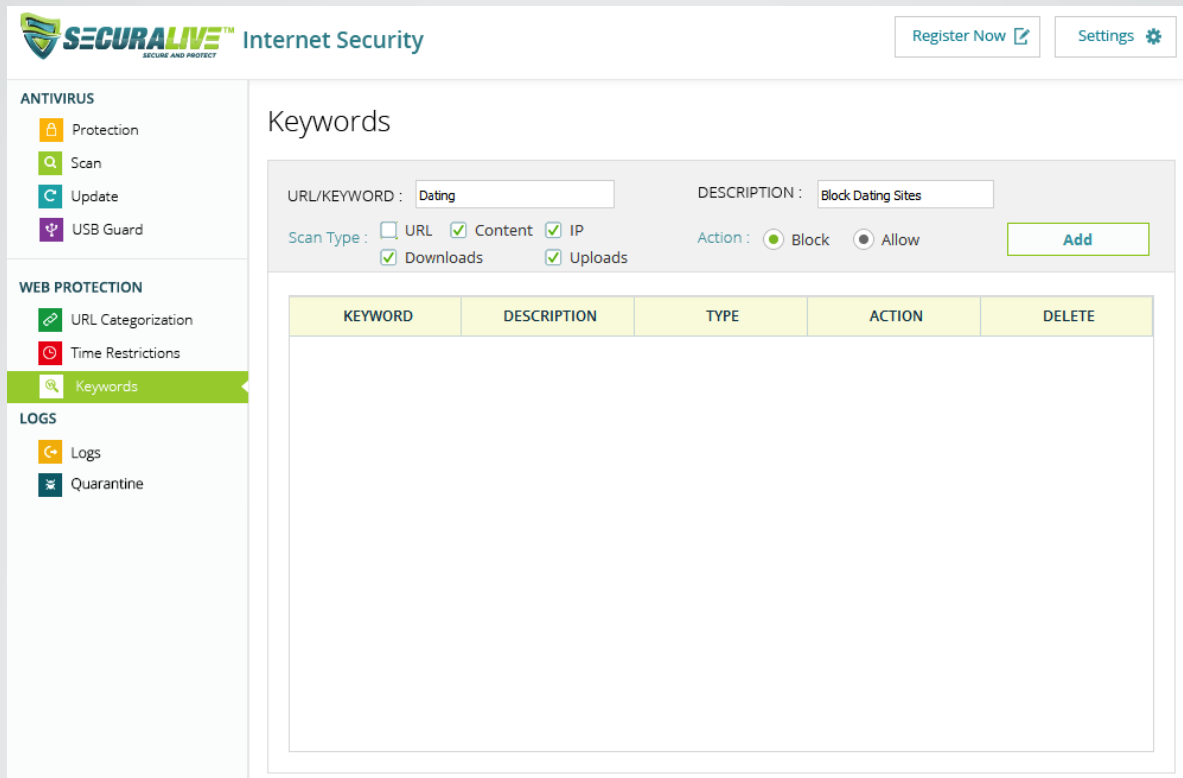
Category Wise BLOCKING & PROTECTION

- You can configure the SecuraLive[®] URL categorization from the application.
- In the application based URL categorization, each row represents one feature. You simply have to check or uncheck checkboxes to enable or disable the features under the Categories section.
- When a check box is checked, then that particular feature is enabled.
- This feature ensures Web applications are used exactly as intended in organizations. It protects against the manipulation of Web environment for malicious intentions and provides an added level of security by the application infrastructure. It has a strong defense against known and emerging hacking attacks and has optimal predefined security rules for instant protection.



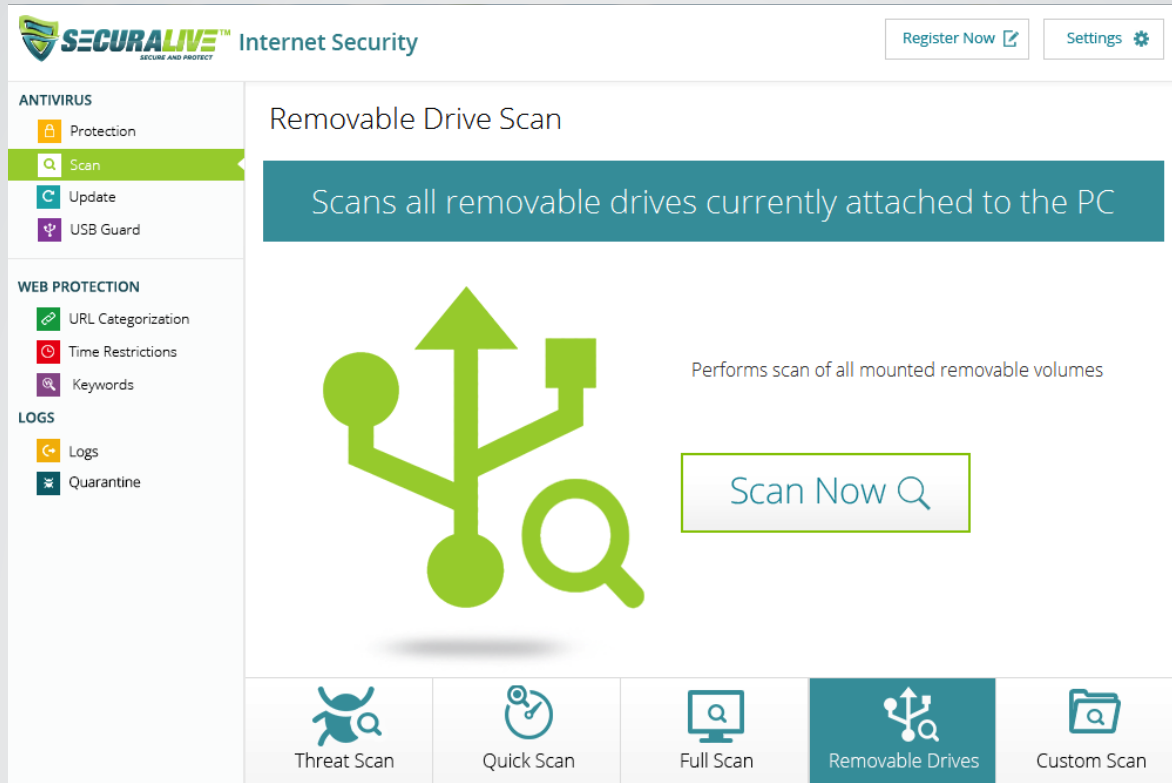
TIME RESTRICTION FEATURES

- SecuraLive® Time Restriction can restrict web access according to a daily time schedule you customize.
- Click “Time Restrictions” in the left-hand column.
- Select all categories or custom and highlight a block of time during which you wish to deny web access. Once you have selected the time (click and drag the mouse), a menu will pop up to block or allow that time.
- Press the “Save” button.
- Repeat until the Time Restrictions fit your needs.
- You can also allow a Time Selection instead of denying it. Note it is a good idea to save changes as you go.



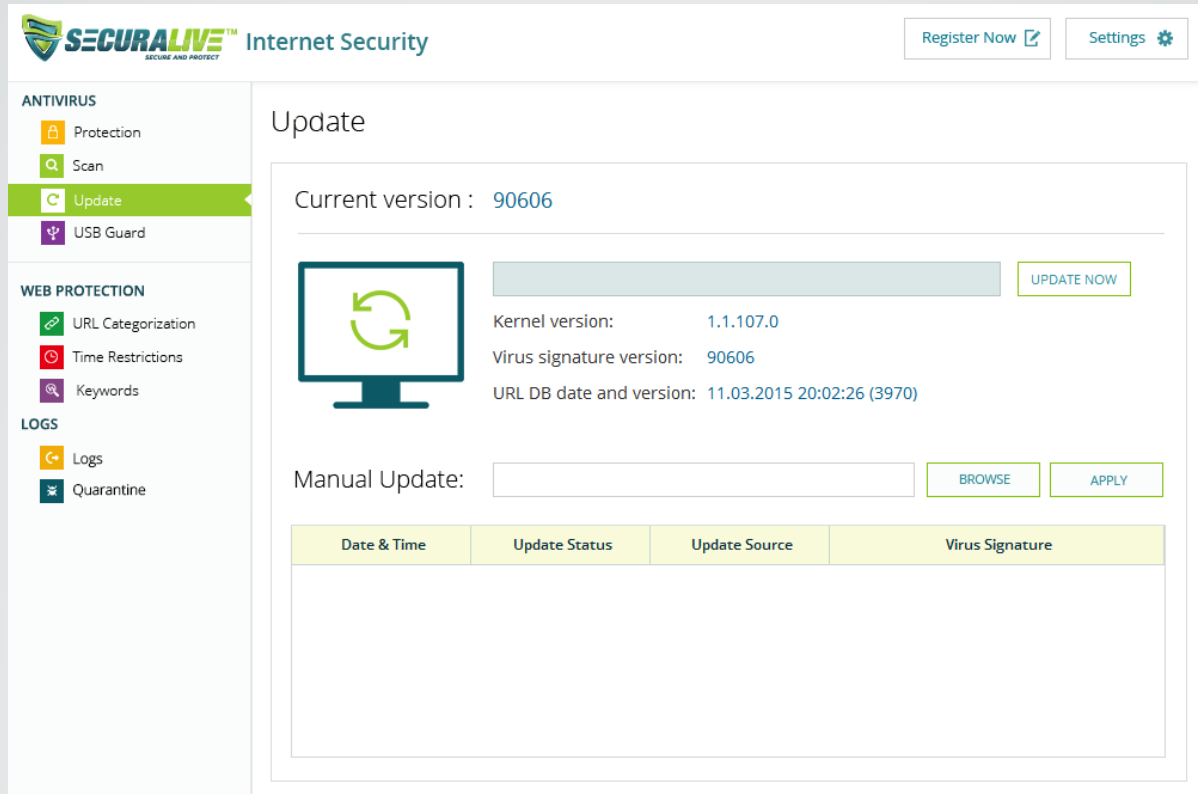
KEYWORD BLOCKING

- Enter a keyword or domain in the Keyword/URL box, fill in the description box and select the match on options, then click “Add”.
- Some examples of Keyword application are: If the keyword “Dating” is specified, the URL <http://www.xxx.com/dating.html> is blocked. If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- To delete a keyword or domain, select it from the list and click “Delete Keyword”.



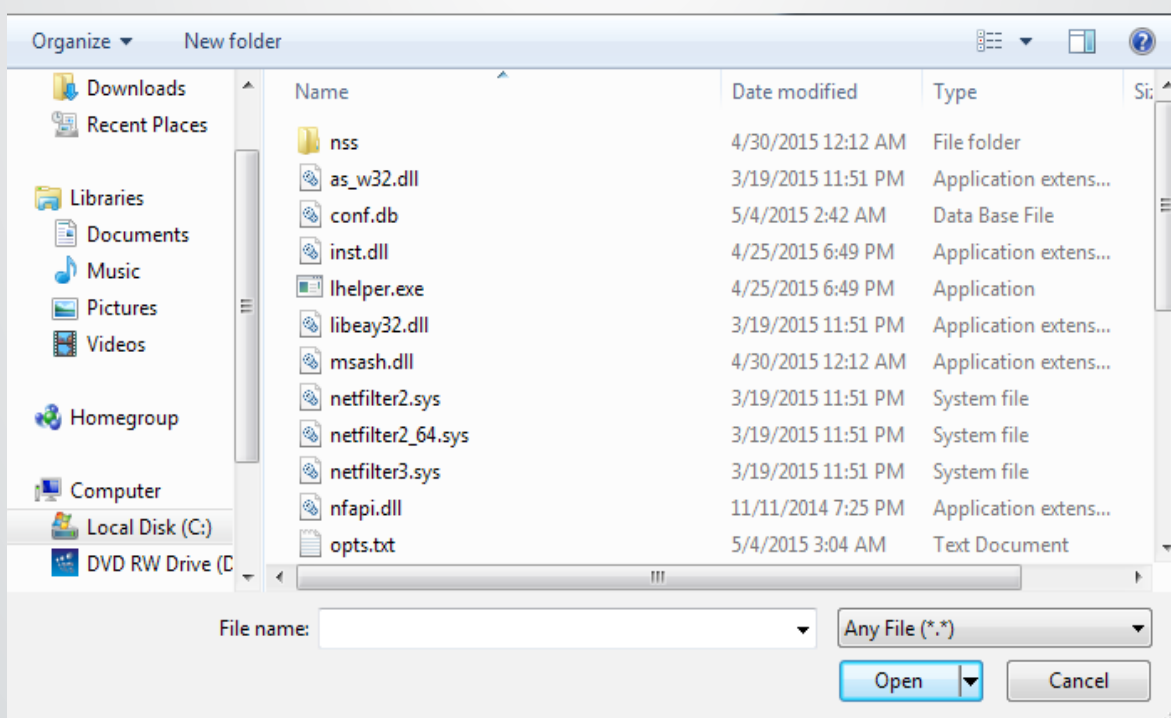
SCAN

- If you want to scan external devices or specific folders in your system then select the “Removable Drives” option.
- Then click on “SCAN NOW”.
- You can also scan the files by right clicking on the file which gives you many options.

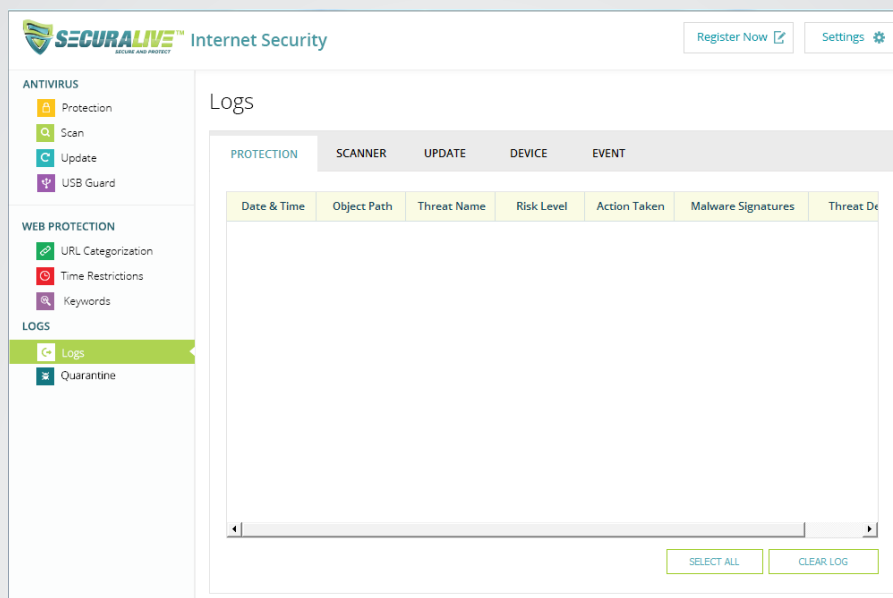


UPDATE

You can also update SecuraLive[®] Internet Security manually. Click on the “Browse” option and find the file location to update and click on “Apply” as shown in the image.



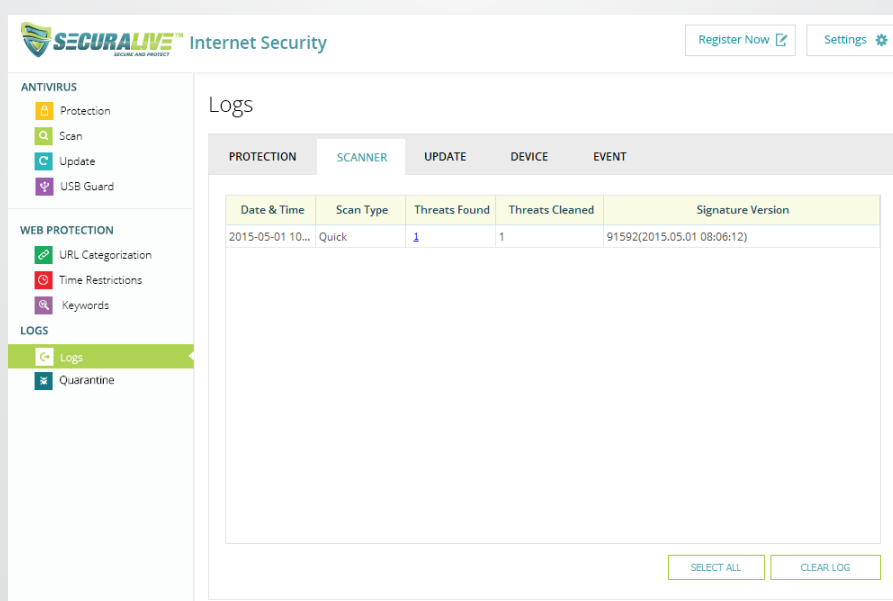
LOGS



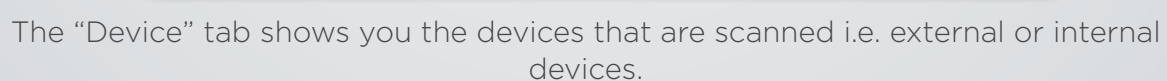
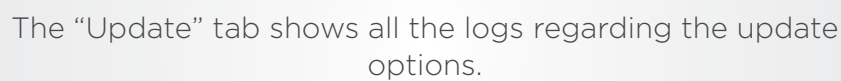
The “Logs” tab shows all the logs regarding the Internet Security functionality.

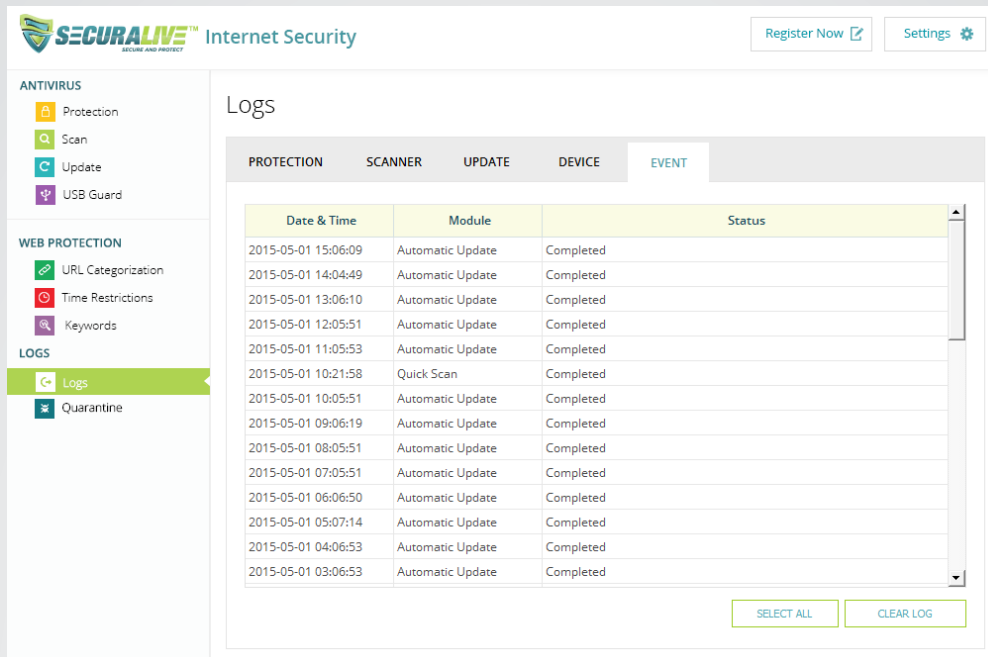
By clicking on each of the 5 tabs as below, you can check out the logs of each tab (“Protection”, “Scanner”, “Update”, “Device”, and “Event”).

The “Protection” tab shows the logs regarding the system’s protection.



The “Scanner” tab logs when the scanning process was carried out and what the current version is etc.

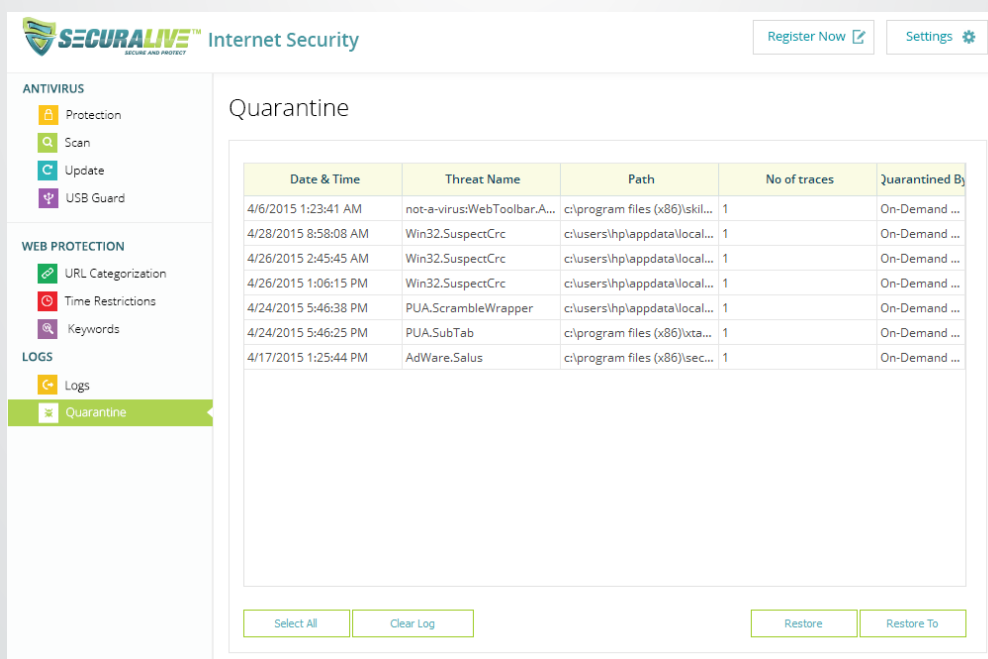




The screenshot shows the SecuraLive Internet Security interface. On the left, there is a sidebar with navigation options: ANTIVIRUS (Protection, Scan, Update, USB Guard), WEB PROTECTION (URL Categorization, Time Restrictions, Keywords), and LOGS (Logs, Quarantine). The 'Logs' option is selected. The main area displays a table titled 'Logs' with tabs for PROTECTION, SCANNER, UPDATE, DEVICE, and EVENT. The 'EVENT' tab is active, showing a list of events with columns for Date & Time, Module, and Status. The events are all 'Completed' and include updates and scans.

Date & Time	Module	Status
2015-05-01 15:06:09	Automatic Update	Completed
2015-05-01 14:04:49	Automatic Update	Completed
2015-05-01 13:06:10	Automatic Update	Completed
2015-05-01 12:05:51	Automatic Update	Completed
2015-05-01 11:05:53	Automatic Update	Completed
2015-05-01 10:21:58	Quick Scan	Completed
2015-05-01 10:05:51	Automatic Update	Completed
2015-05-01 09:06:19	Automatic Update	Completed
2015-05-01 08:05:51	Automatic Update	Completed
2015-05-01 07:05:51	Automatic Update	Completed
2015-05-01 06:06:50	Automatic Update	Completed
2015-05-01 05:07:14	Automatic Update	Completed
2015-05-01 04:06:53	Automatic Update	Completed
2015-05-01 03:06:53	Automatic Update	Completed

The “Event” tab displays the properties, such as whether the scanning process is completed or not and if the current version update has been done manually or automatically etc.



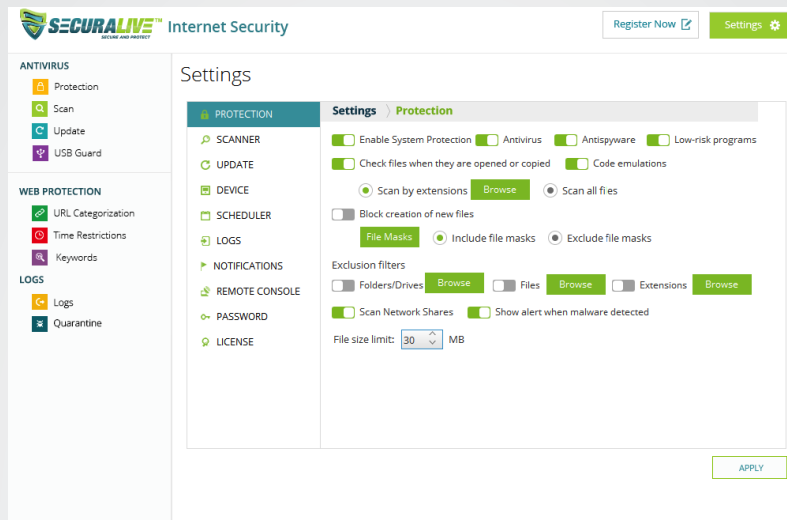
The screenshot shows the SecuraLive Internet Security interface with the 'Quarantine' tab selected. The main area displays a table titled 'Quarantine' with columns for Date & Time, Threat Name, Path, No of traces, and Quarantined By. The table lists several threats that have been quarantined, including 'not-a-virus:WebToolbar.A...', 'Win32.SuspectCrc', and 'PUA.ScrambleWrapper'.

Date & Time	Threat Name	Path	No of traces	Quarantined By
4/6/2015 1:23:41 AM	not-a-virus:WebToolbar.A...	c:\program files (x86)\skil...	1	On-Demand ...
4/28/2015 8:58:08 AM	Win32.SuspectCrc	c:\users\hplappdata\local...	1	On-Demand ...
4/26/2015 2:45:45 AM	Win32.SuspectCrc	c:\users\hplappdata\local...	1	On-Demand ...
4/26/2015 1:06:15 PM	Win32.SuspectCrc	c:\users\hplappdata\local...	1	On-Demand ...
4/24/2015 5:46:38 PM	PUA.ScrambleWrapper	c:\users\hplappdata\local...	1	On-Demand ...
4/24/2015 5:46:25 PM	PUA.SubTab	c:\program files (x86)\xta...	1	On-Demand ...
4/17/2015 1:25:44 PM	AdWare.Salus	c:\program files (x86)\sec...	1	On-Demand ...

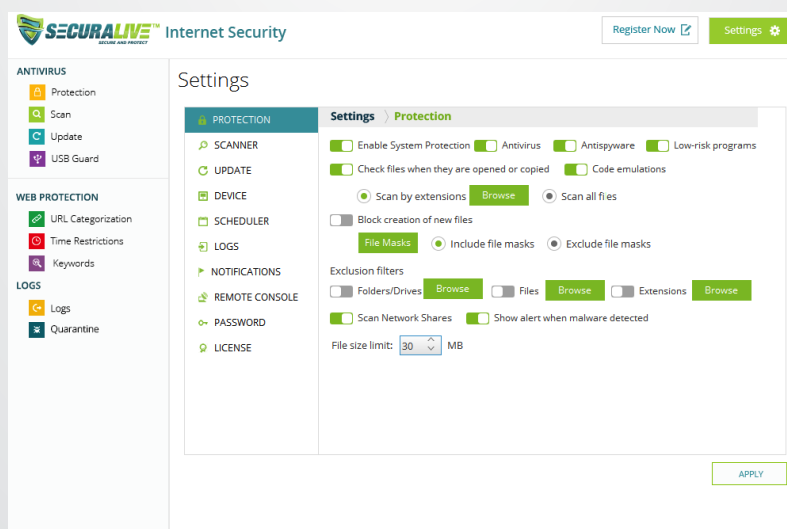
The “Quarantine” tab displays the malicious programs which infect the system, such as trap doors, logic bombs, worms etc.

SETTINGS

PROTECTION



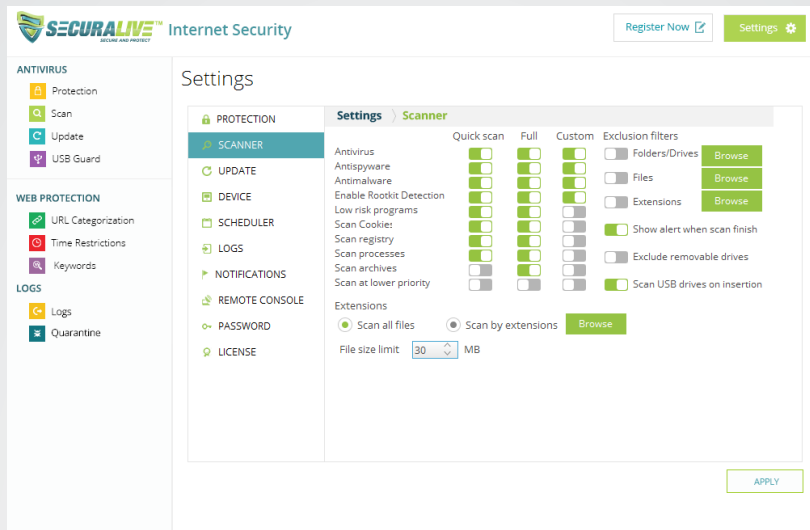
- The wheel symbol on the top right hand corner the “Settings” tab. In the “Protection” tab you are able to enable or disable the scanning options for the devices.
- You can include or exclude the scanning options of the external devices when it is connected to the system.



If you make any changes, then click on “APPLY”.

For example if you disable code emulations, it results in the protection status of code emulations at risk as shown in the image on the left.

SCANNER



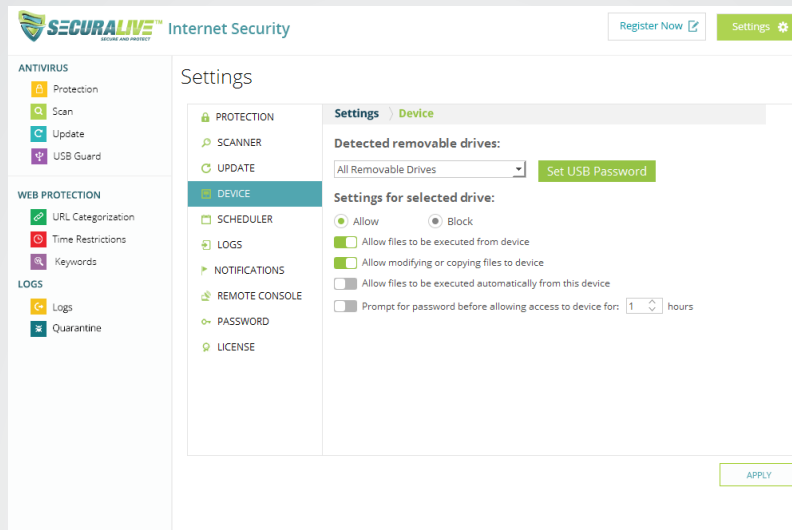
- In the “Scanner” tab, there are lot more options on scanning.
- You can include the extensions to scan automatically when the program is running.
- If you make any changes, then click on “APPLY”.

UPDATE



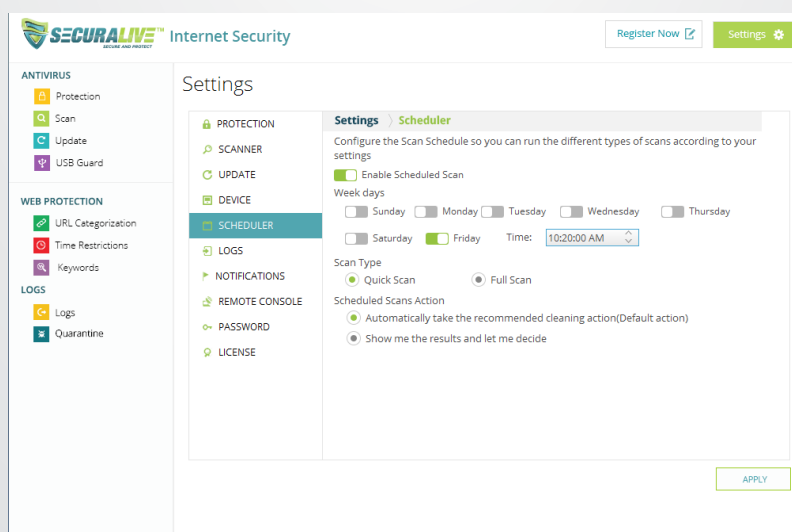
- In the “Update” tab, you can enable or disable the automatic updates.
- You can set the Update source i.e. local or global.
- You can set whether to use the proxy server or not.
- If you make any changes, then click on “APPLY”.

DEVICE



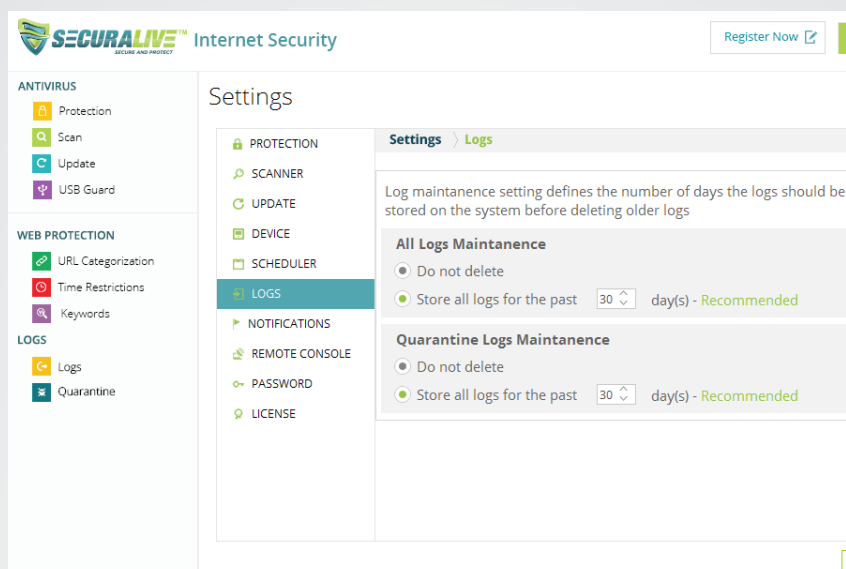
- In the “Device” tab, you can disable or enable the external devices.
- You can give permissions to the external devices.
- If you make any changes, then click on “APPLY”.

SCHEDULER



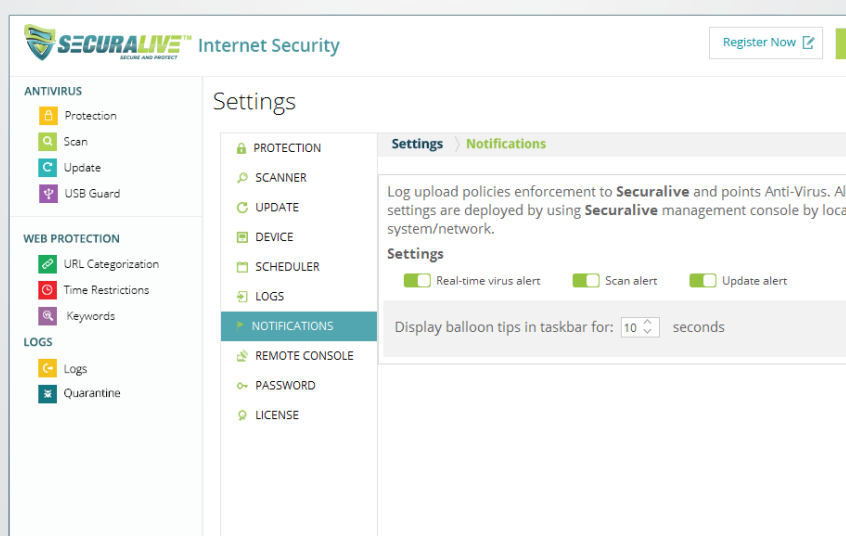
- In the “Scheduler” tab you can schedule when system scanning needs to be carried out. Here you can change the default scanning (full or custom scan).
- If you want to scan your system every day, then select all the days.
- If you make any changes, then click on “APPLY”.

LOGS



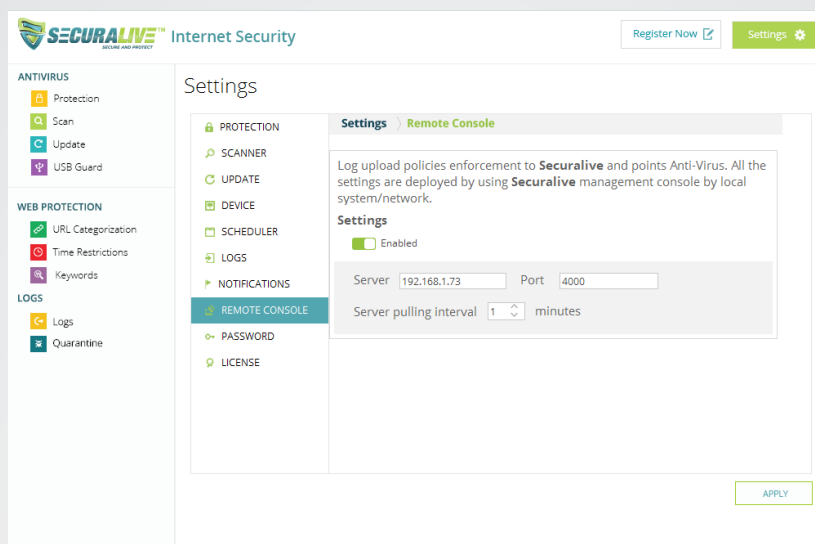
- In the “Logs” tab you can change the settings regarding the logs.
- If you want to delete the logs before 30 days you can set the option to 30 days. We suggest you keep the recommended settings.
- If you make any changes, then click on “APPLY”.

NOTIFICATION



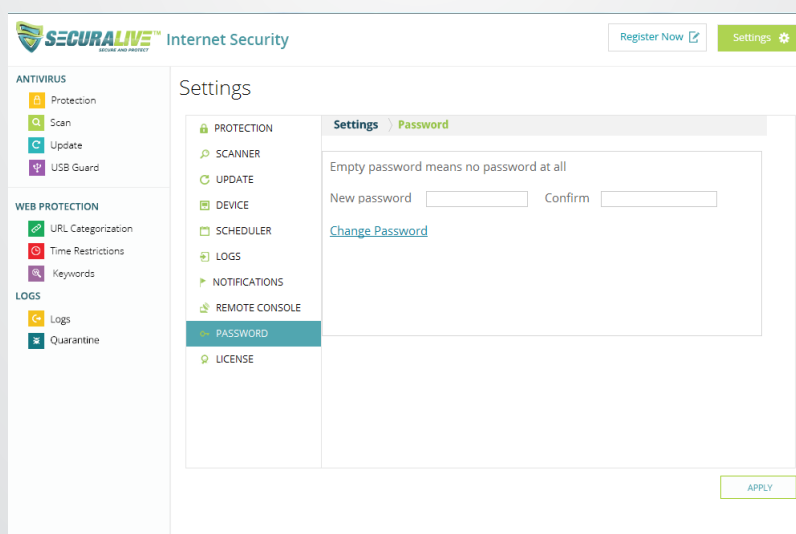
- The “Notification” tab will give alert messages to the user.
- If any malicious program enters the system then it will give an alert message to the user.
- If you make any changes, then click on “APPLY”.

REMOTE CONSOLE



- If your system is in a network and there is a server then the “Remote Console” tab will come into the picture.
- If you have set a server IP and the port number then it will connected to that particular network.
- If you make any changes, then click on “APPLY”.

PASSWORD

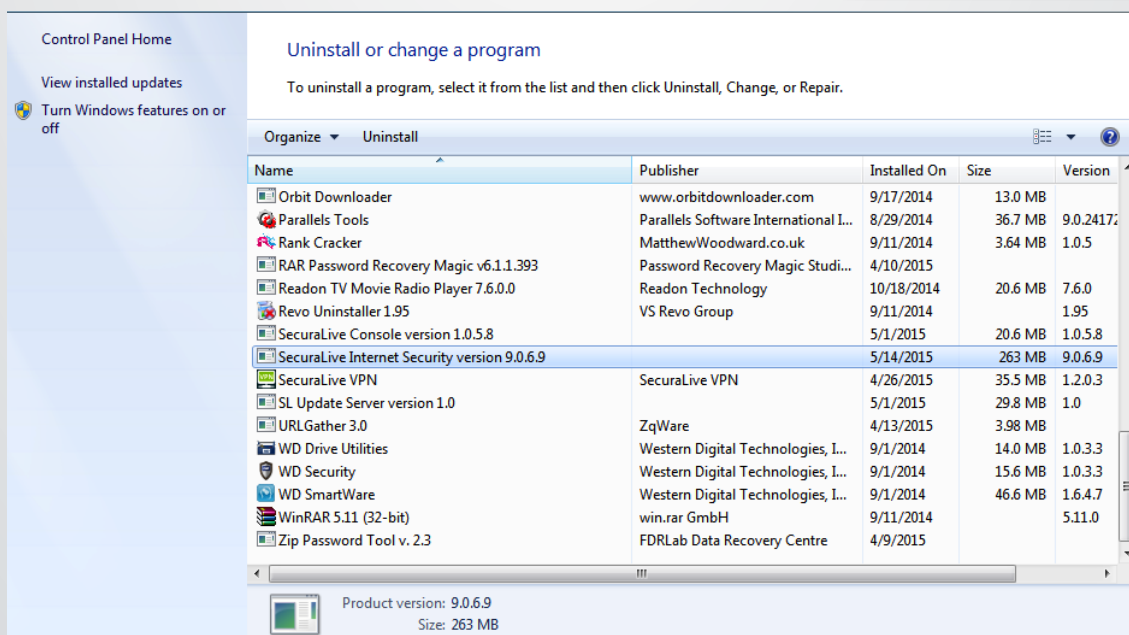
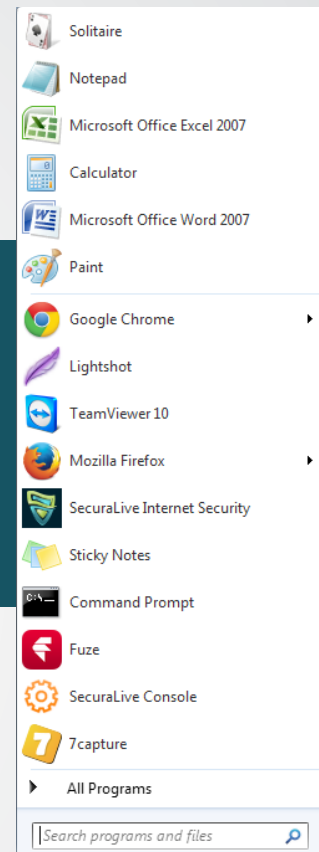


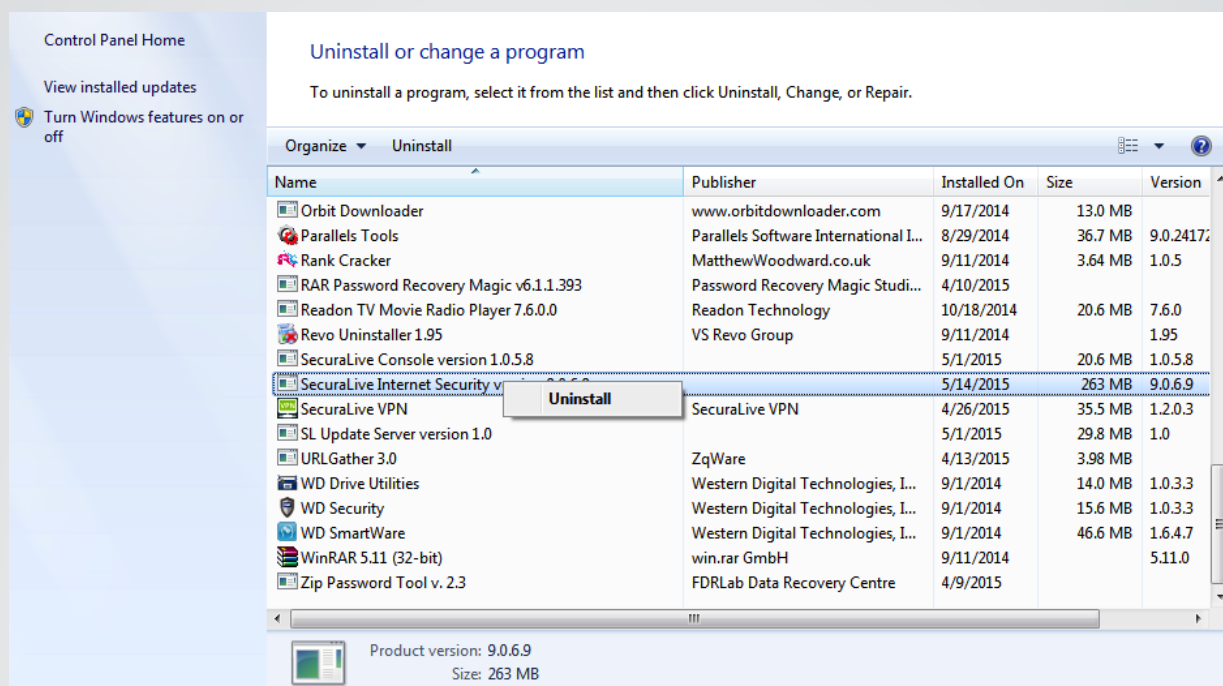
- In the “Password” tab, you can set the password.
- If you set the password then no one can change your settings in SecuraLive® Antivirus.
- The Default password is empty. If you make any changes, then click on “APPLY”.

Uninstalling SecuraLive® INTERNET SECURITY

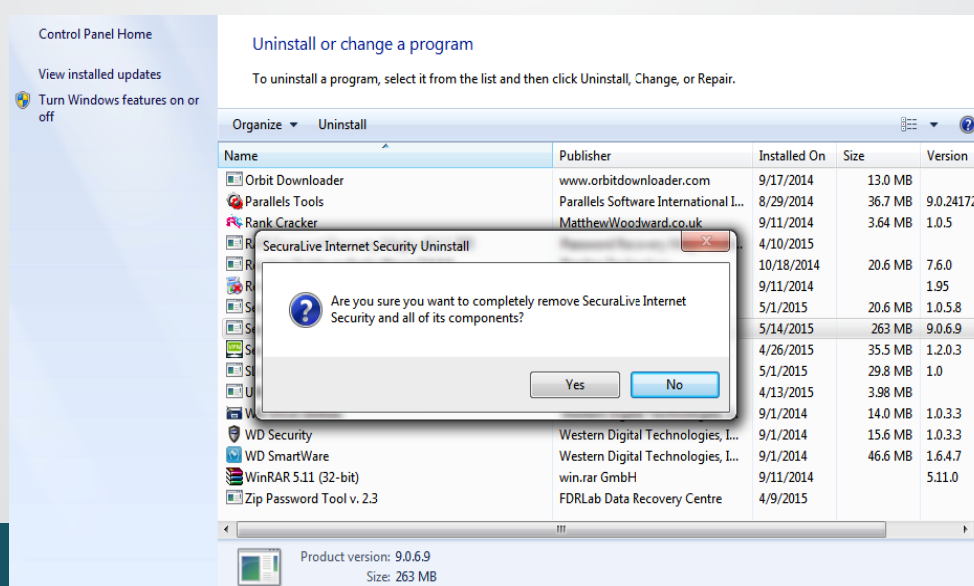
To uninstall the SecuraLive® Antivirus, click on the “Start Menu” button on the taskbar then go to “Control Panel”.

Go to “Programs” as shown above and click on “Uninstall a Program”.

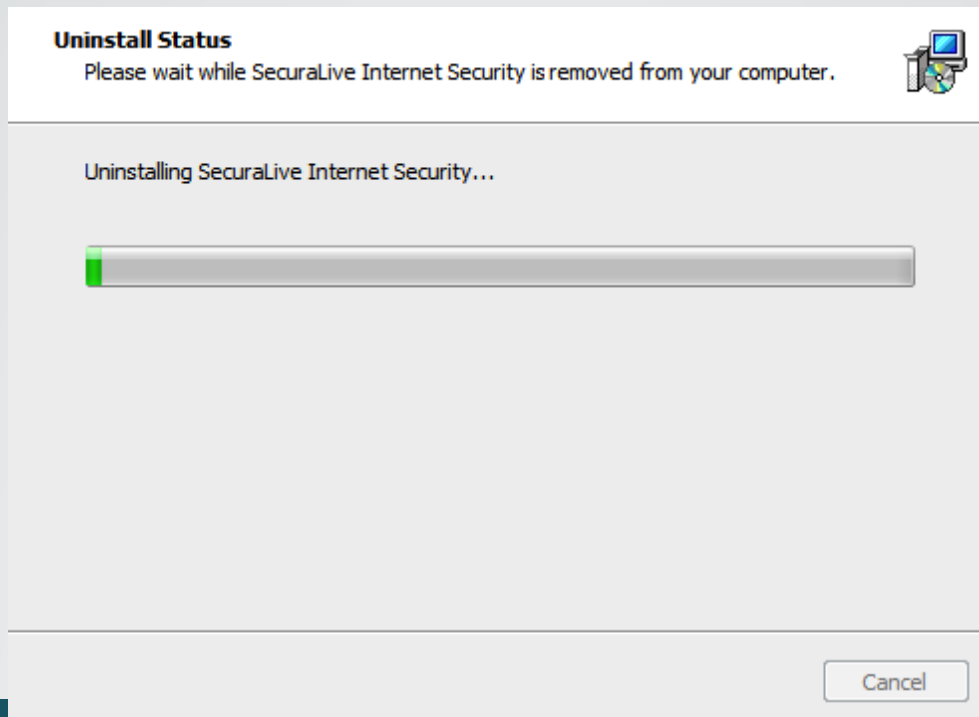




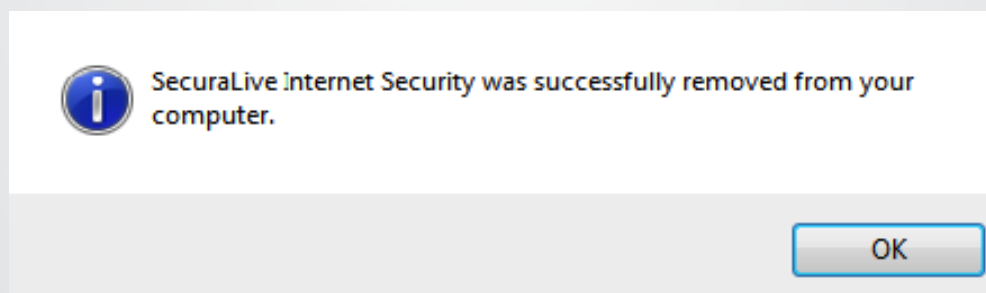
This will navigate you to a list of the system programs that you have installed. Select “SecuraLive® Internet Security Version 9.0.6.9” program and right click. It will then show you the option to uninstall the program as shown in the image.



Click on “Uninstall” and follow the process to uninstall.



Then the process of un-installation will start and continue until the whole green colored bar is filled.



The process of un-installation will start and continue until the whole green colored bar is filled.

Technical Support:

For Technical Support on SecuraLive® Products, please visit
www.securalive.com.

Technical Support is provided either via Live webchat or by submitting a
support ticket on our website.

(c) 2014 - 2015 SecuraLive®, SecuraLive® is a Registered Trademark of PCRange Pty Ltd.
No part of this book may be reproduced or transmitted in any form or by any means, electronic or
mechanical, including photocopying, recording, or by any information storage and retrieval
system, without written permission from SecuraLive®.

Sales: sales@securalive.com
Support: support@securalive.com
Website: www.securalive.com